O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Revista de Direito do Consumidor | vol. 79/2011 | p. 45 - 81 | Jul - Set / 2011
DTR\2011\2474

Laura Schertel Mendes
Mestre em Direito, Estado e Constituição pela UnB. Doutoranda em Direito Privado pela Humboldt-Universität de Berlim (bolsista do Deutscher Akademischer Austauschdienst - DAAD). Foi Coordenadora-Geral de Supervisão e Controle do Departamento de Proteção e Defesa do Consumidor - DPDC do Ministério da Justiça de 2007 a 2010. Pesquisadora do Observatório Brasileiro de Políticas Digitais. Servidora pública federal da carreira de Especialista em Políticas Públicas e Gestão Governamental.

Área do Direito: Constitucional; Consumidor
Resumo: O presente artigo busca rastrear o fundamento constitucional do direito fundamental à proteção de dados pessoais com base na prática jurídica brasileira. A hipótese é a de que o nosso ordenamento pode oferecer instrumentos e conceitos aptos à proteção de dados, se interpretados à luz das modificações sociais e tecnológicas oriundas da sociedade da informação. O artigo está dividido em quatro partes: na primeira, apresenta-se a evolução do conceito de privacidade, demonstrando o desenvolvimento da dimensão da proteção de dados pessoais; na segunda, investiga-se a evolução desse conceito na prática jurídica brasileira por meio do exame jurisprudencial e normativo; na terceira, são apresentados os fundamentos e as características do direito fundamental à proteção de dados pessoais; a última parte traz uma conclusão dos resultados da pesquisa.

Palavras-chave: Direitos fundamentais - Proteção de dados pessoais - Privacidade - Habeas data - Tecnologia
Abstract: The purpose of this article is to demonstrate the basis of the fundamental right to data protection according to the Brazilian Federal Constitution. Our hypothesis is that the Brazilian legal framework offers sufficient instruments and concepts which enables data protection, once its norms are interpreted within the context of information society. This article is divided in four parts: the first one presents the evolution of the right to privacy, highlighting the development of the data protection dimension; the second one investigates the evolution of this right in Brazilian legal experience through the analysis of leading cases and specific ordinary legislation; the third one describes the foundations and features of the fundamental right of data protection; the last part presents the concluding remarks of the present research.

Keywords: Fundamental rights - Data protection - Privacy - Habeas data - Technology
Sumário:

1. Introdução - 2. A evolução do conceito de privacidade - 3. Evidências de um novo conceito de privacidade na prática jurídica brasileira - 4. Fundamentos e características do direito fundamental à proteção de dados: uma análise preliminar - 5. Conclusão - 6. Bibliografia

1. Introdução

Desde a segunda metade do século XX, [1] poucos conceitos jurídicos sofreram tamanha transformação como o conceito envolvendo o direito à privacidade. Da discussão acerca da violação do direito de celebridades fotografadas em situações embaraçosas ou íntimas, o debate sobre o direito à privacidade voltou-se para o risco à personalidade de milhares de cidadãos cujos dados pessoais são coletados, processados e transferidos por organismos estatais e privados, a partir de modernas tecnologias da informação (Simitis, 1986-1987, p. 709 e 710).

Nos mais diversos papéis sociais, como contribuinte, paciente, trabalhador, beneficiário de programas sociais ou como consumidor, o cidadão tem seus dados processados diuturnamente. A vigilância deixa de ser esporádica e torna-se cotidiana.

A utilização massiva de dados pessoais por organismos estatais e privados a partir de avançadas tecnologias da informação apresenta novos desafios ao direito à privacidade. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais (Placzek, 2006, p. 20).

Nesse contexto, destaca-se o surgimento da Internet como uma estrutura aberta de rede de computadores que radicalizou as possibilidades de fluxos de informação de forma inédita. A principal característica da Internet é a sua abertura, tanto em sua arquitetura técnica, como em sua organização social/institucional (Castells, 2003, p. 28 e 29). Essa estrutura aberta da Internet, ao mesmo tempo em que possibilitou a sua difusão e o aperfeiçoamento da tecnologia, propiciou também o desenvolvimento de tecnologias de controle e monitoramento, que podem acarretar a restrição da liberdade do cidadão.

Em razão de modificações sociais e da evolução tecnológica, a discussão sobre os danos causados pelo processamento e fluxo de dados na sociedade não se restringe mais à ameaça do enorme poder do Estado, expresso na figura do *Big Brother de Orwell,* mas abrange hoje também o setor privado, que utiliza massivamente dados pessoais para atingir os seus objetivos econômicos. Assim, a ameaça passa a ser representada pelos "pequenos irmãos" (Buchner, 2006, p. 26), isto é, pelas milhares de empresas que coletam, armazenam e processam dados de seus clientes, consumidores finais ou não. Conforme afirma Hassemer:

"O Estado ainda aparece em algumas áreas (…) em outras, o tema se desloca para distintos demônios, que são muito piores que ele: por meio de uma potente tecnologia da informação nas mãos de qualquer um, essa força se desloca (…) de forma ágil, oculta, voraz e por toda a Terra, coletando, classificando, repreendendo, reunindo, comercializando e utilizando dados pessoais" (1999, p. 131 apud Buchner, 2006, p. 26, trad. livre).

Como afirma Perez Luño, na sociedade atual, a informação converte-se em poder a partir do momento em que a informática permite transformar informações parciais e dispersas em informações em massa e organizadas (1996, p. 43).

Nesse contexto, os riscos à personalidade do cidadão crescem exponencialmente. A violação da privacidade na sociedade da informação passa a significar, por exemplo, o risco do uso indevido de dados pessoais, da classificação dos indivíduos, de imposição de comportamentos padronizados e da discriminação dos cidadãos (Simitis, 1986-1987, p. 710).

O presente artigo objetiva analisar a evolução do conceito de privacidade na experiência jurídica internacional e identificar as evidências da mudança desse conceito na prática jurídica brasileira. Com isso, pretende-se investigar se é possível se falar em um direito fundamental à proteção de dados pessoais no nosso ordenamento jurídico. Trata-se de um estudo inicial, que se insere em uma agenda de pesquisa mais ampla sobre as características e os contornos de um modelo de proteção de dados pessoais apropriado à realidade brasileira.

A hipótese desse artigo é a de que o nosso ordenamento pode oferecer instrumentos e conceitos aptos à proteção de dados, se interpretados à luz das modificações sociais e tecnológicas advindas da sociedade da informação. Para tanto, entendemos relevante analisar a prática jurídica para verificar de que forma o conceito de privacidade tem sido interpretado de modo a resolver os novos desafios apresentados pela sociedade da informação. Assim, o foco deste artigo é uma análise da prática e não da dogmática jurídica, vez que a jurisprudência nacional já conta com bastante profundidade neste tema.

Como método de trabalho, optou-se por pesquisar na jurisprudência e nas normativas legais e infralegais casos em que se reconhece no âmbito do direito à privacidade uma dimensão da proteção de dados pessoais. Escolhemos para essa análise qualitativa os seguintes instrumentos: um acórdão do STF, três acórdãos do STJ, duas leis federais (Código de Defesa do Consumidor (LGL\1990\40) e Lei do Cadastro Positivo) e três decretos presidenciais – o decreto que regula o cadastro único para programas sociais do Governo Federal (Dec. 6.135/2007), o decreto do Serviço de Atendimento ao Consumidor (Dec. 6.523/2008) e o decreto do Censo Anual da Educação (Dec. 6.425/2008).

O artigo está dividido em quatro partes: na primeira parte, apresenta-se a evolução do conceito de privacidade, demonstrando o desenvolvimento da dimensão da proteção de dados pessoais; na segunda, investiga-se a evolução desse conceito na prática jurídica brasileira por meio do exame jurisprudencial e normativo; na terceira, são apresentados, de forma preliminar, os fundamentos e as características do direito fundamental à proteção de dados pessoais; a última parte traz uma conclusão dos resultados da pesquisa.

2. A evolução do conceito de privacidade

O início dos debates doutrinários sobre o direito à privacidade ocorreu como consequência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente impensável. Isso pode ser percebido com o pioneiro artigo sobre privacidade de Warren e Brandeis, intitulado "The right to privacy", [2] no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica (1890, p. 2). A finalidade principal do referido artigo é buscar identificar um direito à privacidade na *common law,* a partir de precedentes jurisprudenciais de tribunais ingleses.

Ao fundamentarem o direito à privacidade, Warren e Brandeis relacionam a sua proteção à inviolabilidade da personalidade, rompendo com a tradição anterior que associava a proteção da vida privada à propriedade. Nas suas palavras, "o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade" (1890, p. 7, trad. livre).

Warren e Brandeis, ao identificarem o direito à privacidade, buscam igualmente definir os seus limites, nos seguintes termos: (a) o direito à privacidade não impede a publicação do que é de interesse geral; (b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito; (c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; (d) o consentimento do afetado exclui a violação do direito; (e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; e (f) a ausência de dolo também não exclui a violação desse direito (1890, p. 12-14).

Como se pode perceber a partir da análise desse artigo, a proteção à privacidade teve um caráter fortemente individualista em seus primórdios, com a sua feição do direito a ser deixado só (*right to be let alone).* É nesse sentido que sobressaíam as suas características de direito negativo, como a exigência absoluta de abstenção do Estado na esfera privada individual para a sua garantia.

No decorrer do século XX, a transformação da função do Estado, aliada à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático (Doneda, 2006). É nesse sentido que se pode afirmar que o século passado vivenciou um "processo de inexorável reinvenção da privacidade" (Rodotà, 2008, p. 15).

Além de adquirir um caráter positivo e de ser reconhecido no âmbito internacional, o direito à privacidade transformou-se, para fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados (Doneda, 2006, p. 27).

A transformação desse conceito pode ser percebida de forma mais clara a partir da década de 70, com a edição de legislações específicas e de decisões judiciais de diversos países, bem como a partir da aprovação de acordos internacionais e transnacionais em diferentes níveis. Todos esses instrumentos compartilham o conceito segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte.

A primeira geração das normas de proteção de dados pessoais surgiu como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas privadas, bem como às ideias de centralização dos bancos de dados em gigantes bancos de dados nacionais (Mayer-Schönberger, 2001). São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o *Fair Credit Reporting Act* (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act* (1974), aplicável à administração pública.

Às legislações nacionais se seguiram importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. Destacam-se, nesse contexto, a Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (1980) e a Diretiva Europeia 95/46/CE relativa à proteção de dados pessoais (1995).

Na evolução do conceito de privacidade, a decisão do Tribunal Constitucional alemão no julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 25.03.1982 é considerada uma referência. [3] Nesse julgamento histórico, o tribunal radicalizou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade e decidiu pela inconstitucionalidade parcial da referida lei, ao argumentar a existência de um direito à "autodeterminação informativa" com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade, respectivamente, art. 1 I GG e art. 2 I GG (BVerfG 65, 1, Censo Demográfico).

A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo à protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação.

A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento. Nesse contexto, argumentou que a Constituição alemã protege o indivíduo contra o indevido tratamento de dados pessoais, por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade.

Nessa formulação de um direito à autodeterminação informativa, a Corte reconheceu uma carga participativa muito maior que a reconhecida pela experiência jurídica em períodos anteriores. Assim, a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre tudo ou nada (Mayer-Schönberger, 2001).

Como se pode perceber, a partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada "privacidade informacional", "proteção de dados pessoais", "autodeterminação informativa", entre outros (Doneda, 2006).

Dessa forma, opera-se na dogmática e na prática jurídica uma clara evolução no direito à privacidade (Rodotà, 2008, p. 17). Primeiramente, ele passa a ser compreendido como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo igualmente uma tutela jurídica coletiva. [4] Em segundo lugar, a privacidade, antes compreendida como o direito negativo de ser em deixado em paz (*right to be let alone*), passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular (BVerfG 65, 1, Censo Demográfico). Por fim, a privacidade, antes ligada exclusivamente a um ideal de liberdade, passa a se vincular também a outros direitos fundamentais, como a igualdade, em razão do crescente risco de discriminação pelo Estado e pelo mercado.

Ao longo do desenvolvimento do conceito de privacidade como proteção de dados pessoais, estabeleceu-se, por meio de instrumentos internacionais e transnacionais, um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados (Bennett, 1992, p. 95). [5] Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados. Uma breve menção a este rol de princípios ajuda a ilustrar a convergência internacional estabelecida neste tema.

Um princípio fundamental que todas as atividades de processamento de dados devem seguir é o *princípio da finalidade,* que indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Esse princípio é essencial para se limitar o acesso de terceiros ao banco de dados. De forma semelhante, ele também serve como parâmetro para julgar se determinado uso dos dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado (Doneda, 2006, p. 216). Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas (Rossnagel, 2003, p. 140).

O *princípio da transparência,* também chamado de *princípio da publicidade,* exige que a existência de um banco de dados pessoais seja de conhecimento público. Ele reafirma o preceito democrático, segundo o qual não podem existir bancos de dados sigilosos e baseia-se na ideia de que a transparência é uma das principais formas de se combaterem os abusos (Bennett, 1992, p. 156). Em contrapartida a esse direito de informação, surge para o banco de dados o dever de publicar seu nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia desse direito. Em alguns países, exige-se autorização estatal prévia ou notificação ao órgão supervisor como pressuposto para o funcionamento dos bancos de dados.

Para possibilitar o controle do titular acerca dos seus dados, outro princípio relevante é o *princípio do consentimento.* Afinal, o exercício da liberdade de controle de dados pessoais baseia-se no consentimento do titular, que pode determinar um maior nível de proteção ou um maior fluxo dos seus dados. Segundo esse princípio, o consentimento deve ser consciente e informado, e apenas situações excepcionais (previstas legalmente) justificam o processamento de dados sem o prévio consentimento do titular.

Outro princípio relevante é o da *qualidade dos dados.*[6] Ele se refere à exigência de que os dados constantes de um banco sejam objeto de um tratamento leal e lícito, sejam adequados pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados. Tal princípio enseja cautela na formação do banco de dados, assim como demanda a sua constante atualização, de forma a impedir que os dados contidos restem ultrapassados com o passar do tempo.

No princípio da qualidade dos dados, incluem-se os *direitos de acesso, retificação e cancelamento dos dados.* O acesso refere-se ao direito do indivíduo de receber a informação acerca dos dados registrados sobre ele, quando assim o requisitar (Cueva, 1990, p. 187). Essa faculdade compreende o conhecimento sobre os dados armazenados, incluindo informações acerca da sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento. O direito de retificação e cancelamento dos dados visa assegurar a qualidade dos dados pessoais, de modo a corrigi-los em caso de equívoco ou cancelá-los, caso estejam obsoletos ou tenham sido indevidamente armazenados. Em caso de correção ou cancelamento dos dados, é direito do indivíduo que todos os organismos que receberam por transferência os seus dados sejam notificados para tomarem as devidas providências.

O *princípio da segurança física e lógica* refere-se à exigência básica de que qualquer banco de dados pessoais esteja protegido contra extravios, destruições, modificações e desvios não autorizados pelos interessados (Doneda, 2006, p. 217). Por fim, um importante princípio da matéria de proteção de dados pessoais é o *princípio da responsabilidade,* que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade.

Como vimos nesta seção, o intenso processamento de dados pelo setor público e privado a partir da década de 70 enseja a evolução do direito à privacidade, que passa a abarcar uma dimensão de proteção de dados pessoais, na qual se destaca o controle do indivíduo sobre o fluxo de suas informações na sociedade. O próximo passo desta pesquisa consiste em investigar se essa evolução também se deu na prática jurídica brasileira. A nossa hipótese é a de que a experiência jurídica no Brasil incorporou uma evolução desse conceito, apesar de não estar acompanhada de uma reflexão ou de um discurso expresso sobre proteção de dados pessoais.

3. Evidências de um novo conceito de privacidade na prática jurídica brasileira

Os desenvolvimentos nas últimas duas décadas da prática jurídica brasileira, tanto no âmbito da jurisprudência, como no âmbito de iniciativas legais e infralegais, sugerem uma evolução do conceito de privacidade também entre nós, inclusive com a aplicação de diversos princípios relacionados à proteção de dados pessoais consolidados na doutrina internacional. A seguir, veremos estes dois aspectos em maior detalhe.

3.1 Jurisprudência

É possível perceber na jurisprudência brasileira desde os anos 90 alguns casos interessantes de assimilação do conceito de privacidade na sua dimensão da proteção de dados pessoais e de autodeterminação informativa.

É interessante iniciar a análise por um acórdão do STF (RHD 22/DF, Pleno, j. 19.09.1991, m.v., rel. Min. Marco Aurélio, rel. p/ acórdão Min. Celso de Mello, *DJ* 01.09.1995), que julga um recurso na ação de *habeas data* proposta em face do extinto Serviço Nacional de Informações – SNI, na qual o impetrante requer o acesso a seus dados pessoais constantes no arquivo daquele órgão. Embora o plenário tenha confirmado a decisão do tribunal de origem, ao decidir, por maioria, pelo desprovimento do *habeas data* em razão da falta de interesse de agir, a análise dos votos dos ministros pode trazer elementos interessantes para o exame da evolução do direito à privacidade, nos termos aqui propostos.

No referido julgamento, pode-se constatar, tanto no voto do Min. Sepúlveda Pertence, que decidiu pelo provimento do recurso, como no voto do Min. Celso de Mello, que entendeu pelo seu desprovimento, a associação do *habeas data* a um direito material de acesso aos dados pessoais protegido pela Constituição.

O Min. Celso de Mello divergiu do relator, Min. Marco Aurélio, ao entender que o recurso não deveria ser provido, por falta de interesse de agir, dada a ausência de pedido administrativo feito pelo requerente, concluindo pela carência da ação de *habeas data.* Não obstante, traz em seu voto importantes contribuições ao relacionar o *habeas data* aos direitos da personalidade, ao direito à intimidade e à esfera de autonomia individual, conforme se percebe no trecho a seguir:

"Discute-se nesta sede recursal, em face do novo ordenamento constitucional, a questão referente à *disclosure of the information,* e à consequente acessibilidade dos registros, informáticos ou não, existentes no extinto Serviço Nacional de Informações (SNI).

Esse tema tem suscitado grande discussão, especialmente porque envolve um dos aspectos mais expressivos da *tutela jurídica dos direitos da personalidade.*

A garantia de acesso a informações de caráter pessoal, registradas em órgãos do estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade" (RHD 22/DF, grifos nossos).

No mesmo sentido, contribuição importante para o tema da privacidade pode ser vista no voto do Min. Sepúlveda Pertence neste mesmo julgamento, que, ao contrário, entendeu configurado o interesse de agir do impetrante de ter acesso aos seus dados pessoais arquivados pelo órgão, nos moldes da doutrina do mandado de segurança. Fundamental para a análise aqui proposta foi a conceituação pelo Min. Sepúlveda Pertence do direito material à proteção de dados pessoais. Segundo ele, a novidade da ação de *habeas data* instituída pela Constituição Federal (LGL\1988\3) reside no direito substancial ao conhecimento dos dados reclamados e não na sua característica processual, conforme se observa no trecho a seguir:

"Penso que tudo isso é de transplantar-se para o *habeas data,* que, a rigor, na modalidade do art. 5.º, LXXII, a,CF/1988 (LGL\1988\3) – isto é, para obter ordem à autoridade para fornecer ao impetrante as informações que sobre ele detenha, efetivamente é, no mínimo, remédio perfeitamente análogo ao mandado de segurança, *cuja novidade não está no perfil processual do instituto, mas, sim, no direito substancial ao conhecimento dos dados reclamados"* (RHD 22/DF, grifos nossos).

Como se pode perceber, a partir da análise dos votos e da ementa [7] do acórdão em questão, o Tribunal associou o *habeas data* não apenas a um direito material à privacidade, mas também a uma ordem democrática transparente, cujo poder não deve se ocultar. Nesse sentido, percebe-se que o entendimento sobre esse instituto guarda mais semelhanças com o debate de proteção de dados pessoais ocorrido na Europa e nos EUA do que à primeira vista poderia se imaginar. Afinal, como já demonstrado, a evolução do conceito de privacidade na sua dimensão de proteção de dados surgiu no contexto internacional com o temor dos cidadãos em relação a um descontrole do poder estatal, a partir dos planos dos governos de centralização dos diversos bancos de dados públicos em um único banco nacional (Garfinkel, 2000; Mayer-Schönberger, 2001; Doneda, 2006). Resta claro, portanto, que também na sua origem, é possível se verificar uma semelhança – o temor frente ao excessivo poder estatal – entre a garantia constitucional de *habeas data* e as mais modernas legislações de proteção de dados internacionais.

Se, por um lado, poder-se-ia argumentar que o *habeas data,* nas suas três dimensões de acesso, correção e complementação de informações, seria por demais restrito, em comparação a um direito à autodeterminação informativa, por outro, resta claro que, na sua essência, o que ele visa a proteger é o mesmo direito material relativo à privacidade dos dados pessoais do cidadão.

Semelhantes indícios de evolução do conceito de privacidade podem ser percebidos também em decisões do STJ, principalmente em conflitos envolvendo os bancos de dados de proteção ao crédito e os desafios impostos pela Internet à privacidade.

Nesse contexto, destaca-se o acórdão proferido no REsp 22.337-9/RS, j. 13.02.1995, de relatoria do Min. Ruy Rosado de Aguiar, que, ao interpretar o art. 43 do CDC (LGL\1990\40), acaba por evidenciar um novo conceito de privacidade.

Trata-se, no caso, de um recurso especial do Clube de Diretores Lojistas que sustenta que a prescrição da ação de cobrança dos débitos que originaram os registros no SPC ocorrerá em 20 anos, nos termos do Código Civil (LGL\2002\400) de 2002, cabendo a manutenção dos registros nos bancos de dados por igual período, e não por cinco anos, conforme previsto no Código de Defesa do Consumidor (LGL\1990\40). A 4.ª Turma não conheceu do recurso, por unanimidade, prevalecendo o entendimento segundo o qual os registros não podem ultrapassar o limite temporal de cinco anos, nos termos do Código de Defesa do Consumidor (LGL\1990\40). A ementa do acórdão tem o seguinte teor:

"Serviço de Proteção ao Crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, § 1.º, do CDC (LGL\1990\40) (Lei 8.078/1990)" (STJ, REsp 22.337-9/RS, 4.ª T., j. 13.02.1995, v.u., rel. Min. Ruy Rosado de Aguiar, *DJ* 20.03.1995).

A análise detalhada do voto do relator, Min. Ruy Rosado de Aguiar, é fundamental para os fins propostos neste artigo, pois a sua argumentação traz inúmeras inovações para o debate do conceito da privacidade, ao extrair consequências da norma sobre banco de dados de proteção ao crédito prevista no Código de Defesa do Consumidor (LGL\1990\40) (art. 43), que até então não tinham sido extraídas pela jurisprudência. Pelo contrário, o debate em torno do art. 43 do CDC (LGL\1990\40), raramente era associado ao direito à privacidade e à proteção de dados pessoais, ficando restrito a uma discussão economicista (importância dos bancos de dados para a redução dos juros do crédito) ou apenas vinculado à violação do direito à honra.

No início de seu voto, o ministro relata o intenso processamento de dados pessoais na sociedade moderna e destaca os riscos advindos dessa atividade, nos seguintes termos:

"A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com plenos conhecimentos de causa, também pode servir, ao Estado ou ao particular para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica" (REsp 22.337-9/RS).

Como se percebe, ao analisar a problemática dos bancos de dados de proteção ao crédito, o Min. Ruy Rosado amplia a sua análise para os riscos do processamento de dados pessoais de uma forma geral. Assim, ele inova na jurisprudência brasileira ao chamar a atenção para os riscos advindos da atividade de processamento de dados, tanto pelo setor público, quanto pelo setor privado. Nas suas palavras, o processamento de dados, quando não utilizado para fins lícitos, poderia acarretar "a devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade" ou possibilitar "ao Estado ou ao particular para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica".

De forma precisa, o julgado acaba por expandir o nosso campo de visão: os termos do voto indicam que o problema aventado é um exemplo em uma miríade de outras tantas formas de processamento de dados na sociedade moderna, que podem causar danos à personalidade dos indivíduos, violar a sua autonomia e reduzir as suas oportunidades econômicas e sociais. Em suma, extrai-se que na sociedade da informação, o processamento de dados é generalizado, pois ocorre "nas múltiplas situações de vida" e, por isso, também os riscos ao cidadão são generalizados.

Uma importante contribuição do acórdão é a percepção da vulnerabilidade do indivíduo em face do processamento de dados pessoais, ao afirmar que "o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo". Ao identificar tal vulnerabilidade, o voto analisado acaba por evidenciar as características desse novo direito à privacidade, necessárias para fazer frente aos desafios da sociedade atual. Sob essa ótica, o direito à privacidade precisa assegurar: (a) transparência do processamento de dados, sem a qual não é possível sequer se proteger contra os riscos do processamento; (b) conhecimento e acesso do titular aos dados armazenados; e (c) possibilidade de correção e cancelamento dos dados.

Outra novidade do julgamento é a associação expressa dos riscos advindos do processamento de dados pessoais com o direito fundamental à inviolabilidade da intimidade e da vida privada, previsto no art. 5.º, X, da CF/1988 (LGL\1988\3), conforme se depreende do seguinte trecho de seu voto:

"A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Na Alemanha, por exemplo, a questão está

posta no nível das garantias fundamentais, com o direito de *autodeterminação informacional (o* cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do *ombudsman,* com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação (Hassemer, *Proteção de dados,* palestra proferida na Faculdade de Direito da UFRGS, 22.11.1993). *'No Brasil, a regra do art.* 5.º, X*, da* CF/1988 (LGL\1988\3)*, é um avanço significativo: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*'" (REsp 22.337-9/RS, grifos nossos).

Assim, pode-se inferir do acórdão o seguinte: (a) o Código de Defesa do Consumidor (LGL\1990\40), em seu art. 43 e em seus princípios, estabelece uma proteção à personalidade e à privacidade do consumidor, também na sua dimensão da proteção de dados pessoais; (b) na sociedade da informação, o processamento de dados pessoais é generalizado, assim como os riscos à personalidade dos cidadãos; (c) para enfrentar esses riscos, é necessário um conceito de privacidade que propicie ao cidadão o controle dos seus dados, como a autodeterminação informativa desenvolvida pela Corte Constitucional alemã; e (d) o art. 5.º, X, da CF/1988 (LGL\1988\3), que determina a inviolabilidade da intimidade e da vida privada, pode se constituir em uma tutela do indivíduo contra os riscos advindos do processamento de seus dados pessoais.

Outro acórdão mais recente do STJ explicita o desenvolvimento de um novo direito à privacidade no nosso ordenamento, a partir de uma discussão sobre a violação da imagem por meio das novas tecnologias, como a Internet (REsp 1.168.547/RJ). Trata-se de recurso especial contra acórdão que obrigou uma empresa ao pagamento de indenização por danos materiais e morais, em razão da divulgação de imagem indevida em página na Internet. A 4.ª Turma do STJ negou, por unanimidade, o recurso especial, nos termos do voto do relator, mantendo a indenização fixada por uso indevido de imagem.

Fundamental no acórdão foi o voto do relator, Min. Luis Felipe Salomão, que após discorrer sobre os novos desafios impostos pela Internet ao ordenamento jurídico, reconhece que as inovações tecnológicas ensejaram o desenvolvimento de um novo conceito de privacidade, pautado no controle da pessoa sobre as próprias informações pessoais, conforme se vê abaixo:

"Contudo, com o desenvolvimento da tecnologia passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, ou seja, o consentimento do interessado é o ponto de referência de todo o sistema de tutela da privacidade" (STJ, REsp 1.168.547/RJ, 4.ª T., j. 11.05.2010, v.u., rel. Min. Luis Felipe Salomão, *DJe* 07.02.2011).

Também a ementa reafirma esse novo conceito de privacidade e a sua autonomia em relação ao contrato firmado:

"10. Com o desenvolvimento da tecnologia, passa a existir um *novo conceito de privacidade,* sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem (…).

13. Ademais, a imputação de utilização indevida da imagem da autora é um *posterius* em relação ao contato de prestação de serviço, ou seja, *o direito de resguardo à imagem e à intimidade é autônomo em relação ao pacto firmado, não sendo dele decorrente.* A ação de indenização movida pela autora não é baseada, portanto, no contrato em si, mas em fotografias e imagens utilizadas pela ré, sem seu consentimento, razão pela qual não há se falar em foro de eleição contratual" (REsp 1.168.547/RJ, grifos nossos).

Nesse sentido, é de se destacar que o conceito firmado no acórdão está em consonância com as mais modernas concepções de privacidade e de proteção de dados pessoais da doutrina internacional. Inclusive, guarda semelhanças marcantes com o conceito de autodeterminação informativa desenvolvido pela Corte Constitucional alemã, conforme explicitado no início deste artigo.

Um último acórdão do STJ ainda merece ser analisado para a demonstração da evolução do conceito de privacidade no direito brasileiro. Trata-se do REsp 306.570/SP de relatoria da Min. Eliana Calmon. O recurso especial foi interposto com a finalidade de obtenção, por meio do Banco Central do Brasil, de informação sobre o atual endereço do réu a partir de dados de contas bancárias, sob o fundamento de que o endereço do réu não estaria acobertado pelo sigilo bancário. A 2.ª Turma do Tribunal não conheceu do recurso, por unanimidade, nos termos do voto da relatora.

De acordo com o voto da Min. Eliana Calmon, não se justifica a requisição ao Banco Central para obtenção do endereço do réu, na medida em que o contribuinte ou o titular tem direito à privacidade em relação aos seus dados pessoais, bem com pelo fato de que cabe à autora efetuar as diligências necessárias para demandar em juízo. Os principais argumentos da Min. Relatora ficaram consubstanciados na ementa do acórdão, que tem o seguinte teor:

"Execução – Requisição de informação de endereço do réu ao Banco Central – Impossibilidade.

1. Embora na hipótese dos autos não se pretenda, através de requisição ao Banco Central, obter informações acerca de bens do devedor passíveis de execução, mas tão somente o endereço, o raciocínio jurídico a ser adotado é o mesmo.

2. *O contribuinte ou o titular de conta bancária tem direito à privacidade em relação aos seus dados pessoais,* além do que não cabe ao Judiciário substituir a parte autora nas diligências que lhe são cabíveis para demandar em juízo.

3. Recurso especial não conhecido" (STJ, REsp 306.570/SP, 2.ª T., j. 18.10.2001, v.u., rel. Min. Eliana Calmon, DJ 18.02.2002 – grifos nossos).

Importante para a análise aqui pretendida é o reconhecimento pelo Tribunal de que uma simples informação, como o endereço do réu, está protegida pelo direito à privacidade, na medida em que é uma informação que se refere a uma pessoa e que a identifica. Ademais, um importante avanço dessa decisão consistiu em estabelecer que a privacidade dos dados pessoais existe de forma independente ao sistema de sigilo bancário, isto é, a não aplicação do sigilo bancário ao caso concreto não acarreta a conclusão de que a informação solicitada é pública ou acessível a todos. Assim, o acórdão inova ao reconhecer a proteção de dados pessoais, para além do binômio sigilo/publicidade.

A partir do exame de casos da jurisprudência do STF e do STJ, é possível extrair conclusões preliminares para a evolução da interpretação do direito à privacidade no nosso ordenamento: (a) a garantia constitucional do *habeas data* estabelece um direito material à proteção de dados pessoais, referente ao conhecimento, correção e complementação dos dados do titular; (b) as modificações sociais e tecnológicas ensejam o desenvolvimento de um novo direito à privacidade no ordenamento jurídico brasileiro, consubstanciado no direito de controle das próprias informações pessoais e no consentimento do seu titular; (c) o direito fundamental à intimidade e à vida privada, previsto no art. 5.º, X, da CF/1988 (LGL\1988\3), protege a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações; (d) uma interpretação conjunta dos art. 5.º, X e LXXII, da CF/1988 (LGL\1988\3), permite, portanto, falar-se em um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro; e (e) o direito fundamental à proteção de dados pessoais opera até mesmo nas situações em que não há sigilo dos dados, pois, como os dados se referem à personalidade do cidadão, estão sob a sua esfera de autonomia.

3.2 Iniciativas legais e infralegais

Após a observação do reconhecimento de um direito à proteção de dados pessoais na jurisprudência nacional, cabe examinar como esse direito se conforma e quais são os seus delineamentos. Como no direito brasileiro, a tutela da privacidade é regulada, além da Constituição Federal (LGL\1988\3), por diversas normas legais e infralegais, a análise desses diplomas pode contribuir para inferirmos quais os princípios que informam a tutela dos dados pessoais no Brasil.

A primeira lei que tratou da privacidade e da proteção de dados pessoais de forma moderna e com vistas a lidar com as novas tecnologias de processamento de dados foi, certamente, o Código de Defesa do Consumidor (LGL\1990\40) (Lei 8.078/1990). Não é por outra razão que ele foi a base de importantes decisões judiciais que explicitaram o direito à proteção de dados, como visto no tópico acima. Não obstante, há diversos outros diplomas que também contemplam a proteção de dados pessoais, como por exemplo, a recém aprovada lei do cadastro positivo (Lei 12.414/2011), o decreto do Serviço de Atendimento ao Consumidor (Dec. 6.523/2008), o decreto que regula o cadastro único para programas sociais do Governo Federal (Dec. 6.135/2007) e o decreto do Censo Anual da Educação (Dec. 6.425/2008).

A seguir, faremos uma análise dessas normas, a fim de examinar de que modo elas regulam a privacidade e a tutela de dados pessoais, bem como avaliar se é possível extrair princípios comuns para essa temática.

O art. 43 do CDC (LGL\1990\40) regula os bancos de dados e cadastros de consumidores, nos seguintes termos:

"Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1.º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2.º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3.º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de 5 (cinco) dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4.º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5.º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores."

Da leitura do dispositivo, depreende-se que o Código autoriza o funcionamento dos bancos de dados e cadastros de consumidores, desde que atendidos determinados preceitos para a proteção da privacidade dos consumidores, quais sejam: (a) possibilidade de acessar todas as informações existentes sobre o consumidor (*direito de acesso*); (b) os dados arquivados devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão (*princípio da qualidade dos dados);* (c) necessidade de comunicação da abertura de cadastro ou registro de dados pessoais de consumo (*princípio da transparência*); (d) obrigação de banco de dados de corrigir os dados de forma imediata (*direito de retificação e cancelamento);* e (e) limite temporal para o armazenamento de dados pessoais (*princípio do*

esquecimento). [8] Como se pode perceber, esse artigo, inspirado nas normas americanas do *National Consumer Act* e do *Fair Credit Reporting Act* (Benjamin; Grinover et al, 2005, p. 400), está em consonância com importantes princípios internacionais de proteção de dados pessoais.

Outro interessante preceito que se extrai desse dispositivo é o conceito segundo o qual *qualquer registro de dados pessoais deve se submeter ao crivo de legalidade,* na medida em que a lei determina que os bancos de dados e cadastros relativos a consumidores são considerados públicos e, portanto, devem respeitar os limites legais. Uma consequência direta dessa norma é que ela enseja também a possibilidade de impetração da ação de *habeas data* contra bancos de dados de consumo. Esse dispositivo acarreta, ao final, a impossibilidade de se argumentar que determinada coleta de dados será utilizada para fins estritamente particulares, não estando submetida à legislação; pelo contrário, qualquer armazenamento de dados pessoais, por se referir à personalidade do consumidor, não diz respeito à esfera privada ou empresarial apenas, mas sim ao público e, portanto, a ele se aplica o regime constitucional e legal.

Passemos agora à análise da recém aprovada Lei 12.414/2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, para formação de histórico de crédito, também conhecida como a lei do cadastro positivo. A sua principal característica reside no fato de ter ampliado a possibilidade do fluxo de dados no mercado, ao possibilitar a formação de bancos de dados com informações de adimplemento, ao mesmo tempo em que buscou estabelecer regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade. Em razão da complexidade e dimensão da lei, não será possível neste espaço discorrer detalhadamente sobre as suas normas. Antes, buscar-se-á extrair os principais preceitos nela previstos que demonstram uma preocupação com a tutela da privacidade e dos dados dos titulares. [9]

Nos moldes do Código de Defesa do Consumidor (LGL\1990\40), a lei estabelece o *princípio da qualidade dos dados pessoais* (art. 3.º, § 1.º, da Lei 12.414/2011), bem como *os direitos de acesso, retificação e cancelamento dos dados* (art. 5.º, II e III, Lei 12.414/2011). Além disso, ela delimita *a finalidade* pela qual os dados podem ser coletados e usados (arts. 2.º, I, 5.º, VII, e 7.º, da Lei 12.414/2011), ao determinar que as informações armazenadas nos bancos de dados somente poderão ser utilizadas para a "realização de análise de risco de crédito do cadastrado" ou para "subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente". Nesse sentido, resta clara a vedação desses dados para *marketing* direto ou qualquer outra atividade não mencionada na lei.

É de se destacar também que a referida lei consolida a evolução de um conceito de autodeterminação informativa no nosso ordenamento, ao estabelecer mecanismos de controle do indivíduo sobre os seus dados, atribuindo a ele o poder de decidir se tem interesse ou não em formar esse histórico e de decidir quando deseja cancelá-lo. É o que se depreende dos seguintes dispositivos que erigem o *princípio do consentimento à* pedra de toque do sistema do cadastro positivo:

"Art. 4.º A abertura de cadastro requer *autorização prévia* do potencial cadastrado mediante *consentimento informado* por meio de assinatura em instrumento específico ou em cláusula apartada (…).

Art. 5.º São direitos do cadastrado:

I – obter o *cancelamento do cadastro quando solicitado;*

(…).

Art. 9.º O compartilhamento de informação de adimplemento só é permitido se *autorizado expressamente pelo cadastrado,* por meio de assinatura em instrumento específico ou em cláusula apartada" (grifos nossos).

Como se percebe, trata-se de um conhecido preceito constitucional, que passa a ser explicitado nessa lei: a Constituição, ao estabelecer a privacidade como direito fundamental, assegura ao cidadão a autodeterminação e o controle do fluxo dos seus dados pessoais na sociedade. Dessa forma, a titularidade dos dados pessoais do cidadão não pode ser transferida, cabendo somente a ele decidir sobre o destino dos seus dados.

Muito importante para a presente análise é o reconhecimento explícito do *princípio da proibição do armazenamento de informações sensíveis e excessivas,* nos termos do art. 3.º, § 3.º, da Lei 12.414/2011. Tal proibição baseia-se no fato de que o processamento de alguns tipos de informações (como, por exemplo, a informação sobre origem social e étnica, saúde, informação genética, orientação sexual e convicções políticas, religiosas e filosóficas) pode acarretar a discriminação do cidadão na sociedade, violando o princípio da igualdade.

Inovador, na lei ora analisada, foi o reconhecimento do preceito do art. 5.º, VI, que prescreve ao titular o direito de "solicitar ao consulente a revisão de *decisão realizada exclusivamente por meios automatizados*" (grifos nossos). Trata-se de uma regra de justiça, que visa assegurar a possibilidade de defesa do titular e a sua participação em um processo de decisão tomado com base em seus dados e que afetará de forma significativa as suas oportunidades de vida. [10]

O art. 16 da Lei 12.414/2011, também consolida um entendimento há muito pacificado no nosso ordenamento, segundo o qual os danos materiais e morais causados pelas atividades de risco devem ser reparados no âmbito de um *sistema de responsabilidade objetiva e solidária.*

Por fim, vale mencionar que um importante conceito reafirmado pela Lei 12.414/2011 foi o da necessidade de *controle da atividade de processamento de dados por autoridade administrativa,* de modo a se ter um sistema administrativo de fiscalização e resolução de conflitos em conjunto com um sistema clássico judicial de solução de lides. Esse princípio está consubstanciado no art. 17 da Lei 12.414/2011, que tem o seguinte teor:

"Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei 8.078, de 11 de setembro de 1990 – Código de Proteção e Defesa do Consumidor (LGL\1990\40), aplicam-se as sanções e penas nela previstas e o disposto no § 2.º.

§ 1.º Nos casos previstos no *caput,* a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa.

§ 2.º Sem prejuízo do disposto no *caput* e no § 1.º, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas, estabelecendo aos bancos de dados que descumprirem o previsto nesta Lei obrigações de fazer com que sejam excluídas do cadastro, no prazo de 7 (sete) dias, informações incorretas, bem como cancelados cadastros de pessoas que não autorizaram a abertura."

Se passarmos agora para a análise das normas infralegais, veremos que é possível identificar, em três decretos sobre temas distintos, a preocupação com o *princípio da finalidade.* Trata-se do preceito segundo o qual o tratamento de dados pessoais somente pode ser realizado para a mesma finalidade pela qual os dados foram coletados. É o que se chama também de *princípio da não descontextualização,* uma vez que os dados coletados legitimamente para uma determinada finalidade, se usados fora de contexto, podem acarretar danos à personalidade do titular.

A generalidade desse princípio para a temática da privacidade, na sua dimensão da proteção de dados, enseja a sua aplicação aos mais diversos temas, como nos casos ora analisados: decreto do Serviço de Atendimento ao Consumidor (Dec. 6.523/2008), decreto do Censo Anual da Educação (Dec. 6.425/2008) e decreto que regula o cadastro único para programas sociais do Governo Federal (Dec. 6.135/2007). Vejamos de que forma esse princípio está redigido em cada uma dessas normas.

O Dec. 6.523/2008, que regula o Serviço de Atendimento ao Consumidor – SAC, em seu art. 11, prescreve que os dados registrados no SAC somente podem ser utilizados para fins de atendimento ao consumidor e que devem ser mantidos em sigilo. O referido artigo tem o seguinte teor:

"Art. 11. Os dados pessoais do consumidor serão preservados, mantidos em sigilo e *utilizados exclusivamente para os fins do atendimento"* (grifos nossos).

A lógica do artigo é facilmente compreendida: ora, se o próprio decreto obriga a empresa ao arquivamento das gravações e dos registros telefônicos para propiciar meios de defesa ao consumidor e formas de fiscalização do Estado (art. 15, § 3.º e 4.º, do Dec. 6.523/2008), é legítimo que esses dados não possam ser utilizados para nenhuma outra finalidade alheia ao serviço de atendimento ao consumidor.

De forma análoga, o Dec. 6.425/2008, que normatiza o censo escolar, também faz uso do princípio da finalidade, ao determinar que os dados do censo não podem ser utilizados para fins estranhos aos da legislação educacional, além de mencionar expressamente a proteção dos dados pessoais, nos seguintes termos:

"Art. 6.º Ficam assegurados o sigilo e a *proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para fins estranhos aos previstos na legislação educacional aplicável"* (grifos nossos).

Outro caso explícito de menção ao princípio da finalidade é o Dec. 6.135/2007, que regula o cadastro único para programas sociais do Governo Federal. Tendo em vista a complexidade dos dados e a sensibilidade das informações nele registradas, é possível perceber que a regulação sobre o processamento, a transferência e a utilização dos dados é mais extensa do que nos diplomas anteriores. [11] Vejamos o teor do art. 8.º:

"Art. 8.º Os dados de identificação das famílias do CadÚnico *são sigilosos e somente poderão ser utilizados para as seguintes finalidades:*

I – formulação e gestão de políticas públicas; e

II – realização de estudos e pesquisas.

§ 1.º São vedadas a cessão e a utilização dos dados do CadÚnico *com o objetivo de contatar as famílias para qualquer outro fim que não aqueles indicados neste artigo.*

§ 2.º A União, os Estados, os Municípios e o Distrito Federal poderão utilizar suas respectivas bases *para formulação e gestão de políticas públicas* no âmbito de sua jurisdição.

§ 3.º O Ministério do Desenvolvimento Social e Combate à Fome poderá ceder a base de dados nacional do CadÚnico para sua utilização, por órgãos do Poder Executivo Federal, em políticas públicas que não tenham o CadÚnico como instrumento de seleção de beneficiários.

§ 4.º Os dados a que se refere este artigo somente poderão ser cedidos a terceiros, para as finalidades mencionadas no *caput,* pelos órgãos gestores do CadÚnico no âmbito da União, do Distrito Federal e dos Municípios.

§ 5.º A utilização dos dados a que se refere o *caput* será pautada pelo respeito à *dignidade do cidadão e* à *sua privacidade.*

§ 6.º A utilização indevida dos dados disponibilizados acarretará a *aplicação de sanção civil e penal na forma da lei"* (grifos nossos).

Como se percebe, em primeiro lugar, a norma explicita que os dados estão restritos à utilização para fins de políticas públicas ou para a realização de estudos e pesquisas. Ou seja, qualquer outra finalidade não prevista está proibida pelo decreto. Em segundo lugar, a norma veda expressamente a utilização dos dados para o contato com os cadastrados, para fins alheios ao mencionado no *caput.* Isto é, proíbe-se claramente a realização de *marketing* ou publicidade com base nos dados do cadastro único. Por fim, o dispositivo invoca preceitos constitucionais – a privacidade e a dignidade – como fundamentos da utilização dos dados, ressaltando que a sua utilização indevida ocasionará a aplicação das sanções cabíveis.

Nos três casos, constata-se que os decretos não proíbem o tratamento dos dados pessoais; ao contrário, exatamente por reconhecer a necessidade da utilização desses dados de forma legítima, é que essas normas propiciam o processamento dos dados, com limitações expressas. Se assim não fosse, haveria o risco de que o tratamento legítimo de dados acabasse se transformando em um tratamento ilegítimo, caso o princípio da finalidade não fosse respeitado. Dessa forma, percebe-se que o direito à proteção de dados pessoais constitui um meio de propiciar segurança jurídica para o fluxo de dados numa sociedade da informação, ao mesmo tempo em que protege a personalidade e a dignidade da pessoa.

Como se pode perceber, tanto a partir da análise jurisprudencial, como do exame de normativas legais, é possível afirmar que há, atualmente, no direito brasileiro um conceito de proteção de dados pessoais, no qual está consubstanciada grande parte dos modernos princípios de privacidade já consolidados internacionalmente. Trata-se de um desenvolvimento natural do direito à privacidade, em resposta às novas demandas originadas na sociedade da informação.

3.3 Resultados preliminares

Nesta seção, visa-se reunir de forma sucinta os principais resultados encontrados na pesquisa até agora. A partir da análise jurisprudencial e normativa, é possível extrair algumas conclusões a respeito da evolução da interpretação do direito à privacidade no nosso ordenamento. Longe de esgotar as suas características, trata-se de apontamentos preliminares sobre os contornos da proteção de dados pessoais na experiência jurídica brasileira:

(a) na sociedade da informação, o processamento de dados pessoais é generalizado, assim como os riscos à personalidade dos cidadãos;

(b) para enfrentar esses riscos, é necessário um conceito que propicie ao cidadão o controle dos seus dados, como a autodeterminação informativa desenvolvida pela Corte Constitucional alemã;

(c) as modificações sociais e tecnológicas ensejam o desenvolvimento de um novo direito à privacidade no ordenamento jurídico brasileiro, consubstanciado no direito de controle das próprias informações pessoais e no consentimento do seu titular;

(d) o direito fundamental à inviolabilidade da intimidade e da vida privada, previsto no art. 5.º, X, da CF/1988 (LGL\1988\3), protege a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações;

(e) a garantia constitucional do *habeas data* estabelece um direito material à proteção de dados, consubstanciado no direito ao conhecimento, correção e complementação dos dados do titular;

(f) uma interpretação conjunta dos incs. X e LXXII do art. 5.º da CF/1988 (LGL\1988\3), permite, portanto, falar-se em um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro;

(g) a proteção de dados pessoais opera até mesmo nas situações em que não há sigilo dos dados, pois, por se referirem à personalidade do cidadão, estão sob a sua esfera de autonomia;

(h) o direito fundamental à proteção de dados pessoais deve-se pautar no cumprimento dos seguintes princípios: *finalidade, esquecimento, qualidade dos dados, transparência e consentimento;*

(i) a concretização do direito fundamental à proteção de dados pessoais exige que o titular tenha efetivo controle sobre a circulação dos seus dados na sociedade, o que somente pode ser alcançado por meio da garantia dos seguintes direitos: *direito geral de informação, amplo direito de acesso aos dados, direito de notificação, direito de retificação, cancelamento e bloqueio dos dados;*

(j) a proteção do indivíduo contra a discriminação pelo processamento dos dados pessoais somente pode ser atingida com a garantia do *direito de não se ficar sujeito a uma decisão individual automatizada,* bem como com a *proibição ou limitação do armazenamento de informações sensíveis e excessivas;*[12]

(l) a efetivação do direito fundamental à proteção de dados depende do *controle e fiscalização da atividade de processamento de dados por autoridade administrativa,* de modo a complementar um sistema judicial de resolução de conflitos; e

(m) para a reparação dos danos morais e materiais advindos da violação do direito fundamental à proteção de dados, faz-se necessária a constituição de um *sistema de responsabilidade objetiva e solidária.*

A análise normativa e jurisprudencial realizada nesta seção evidenciou o reconhecimento de um direito à proteção de dados pessoais na prática jurídica brasileira. Mais do que isso, indicou também que as manifestações desse direito pautam-se num conjunto comum de princípios, que estão em consonância com a experiência internacional de proteção de dados. Na próxima seção, veremos quais são os fundamentos desse direito na Constituição Federal (LGL\1988\3).

4. Fundamentos e características do direito fundamental à proteção de dados: uma análise preliminar

Neste tópico impende apreciar quais são as bases para o direito fundamental à proteção de dados na Constituição Federal (LGL\1988\3), o que justifica uma evolução desse conceito e quais são as consequências do reconhecimento desse direito fundamental.

Como visto anteriormente, com o advento da sociedade da informação, surgem importantes desafios para o ordenamento jurídico e os seus intérpretes, especialmente para a proteção da personalidade e da vida privada do indivíduo. Para possibilitar a resposta adequada aos desafios sociais atuais, é fundamental que a teoria do direito se reconstrua e se reinterprete a ponto de compreender e solucionar os novos problemas enfrentados pelo homem na era da informação (Perez Luño, 1996, p. 10).

Esse desafio se apresenta de forma ainda mais premente no nível constitucional. Afinal, a vitalidade e a continuidade da Constituição dependem da sua capacidade de se adaptar às novas transformações sociais e históricas, possibilitando uma proteção dos cidadãos contra novas formas de poder que surgem na sociedade. [13] Nesse aspecto reside uma tensão inerente ao conceito de Constituição: de um lado, ela deve expressar continuidade, permanência, segurança e estabilidade, de outro, deve exprimir flexibilidade, abertura de interpretação e atualização para a constante concretização dos direitos e princípios nela consagrados. O paradoxo consiste no fato de que a continuidade da Constituição somente é possível se "nela o passado e o futuro se vincularem" (Häberle, 1978, p. 61 e 62).

Assim, é sob a perspectiva de uma compreensão dinâmica da Constituição, [14] como um projeto inacabado e sujeito a alterações interpretativas que refletem um processo de aprendizagem falível, que é preciso interpretar o direito à privacidade na Constituição Federal (LGL\1988\3). [15]

A análise jurisprudencial e normativa demonstrou que já existe uma rica experiência institucional em curso, há mais de duas décadas, que reconhece a evolução do conceito de privacidade, de modo a abarcar a proteção dos dados pessoais do cidadão no nosso ordenamento jurídico. A partir dessas experiências e da vivência institucional relacionada à proteção de dados no Brasil, entendemos que hoje é possível se reconhecer um direito fundamental à proteção de dados pessoais, como uma dimensão da inviolabilidade da intimidade e da vida privada, nos termos da Constituição.

Ao prescrever a inviolabilidade da intimidade e da vida privada, em seu art. 5.º, X, a Constituição Federal (LGL\1988\3) não restringe a aplicação desse conceito a nenhuma situação específica. Isto é, depreende-se desse dispositivo uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentido excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais.

Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais", que ensejaram o nascimento desse direito, como a hipótese de ser flagrado por paparazzi ou de ser notícia de jornais sensacionalistas. Assim, se é consenso que a Constituição Federal (LGL\1988\3) protege o homem médio desses riscos, que raramente ocorrerão na vida real, não haveria sentido em negar--lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.

Entendemos que a menção de dois termos pela Constituição Federal (LGL\1988\3), ao prescrever a "inviolabilidade da *intimidade* e da *vida privada*", não altera os resultados aqui apresentados. Pelo contrário, uma rápida análise de alguns instrumentos internacionais de proteção de dados demonstra que a sua nomenclatura coincide com a da nossa Constituição. Vejamos, por exemplo, a Convenção 108 do Conselho da Europa – Convenção para a proteção das pessoas, em relação ao tratamento automatizados de dados pessoais, que se refere expressamente à "proteção da vida privada" ao declarar o seu objetivo:

"Art. 1.º Objetivos e finalidades

A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, *e especialmente pelo seu direito à vida privada,* face ao tratamento automatizado dos dados de caráter pessoal que lhes digam respeito ('protecção dos dados')" (grifos nossos).

O mesmo se dá com a Diretiva Europeia 95/46/CE sobre proteção de dados pessoais:

"Art. 1.º Objetivo de directiva

1. Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

Para além da coincidência do léxico com os modernos instrumentos internacionais de tutela da privacidade, certo é que a inviolabilidade da intimidade e da vida privada numa sociedade da informação somente pode ser atingida hoje por meio da proteção de dados pessoais. Assim, quando se interpreta a norma do art. 5.º, X, em conjunto com a garantia processual do *habeas data,* é possível extrair-se da Constituição Federal (LGL\1988\3) um verdadeiro direito fundamental à proteção de dados pessoais.

Entendemos que o reconhecimento desse direito fundamental não é apenas uma possibilidade; trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal (LGL\1988\3).

À luz desse entendimento, verifica-se que a Constituição apresenta dois importantes mecanismos de tutela da personalidade contra o tratamento indevido de dados: o direito material à proteção de dados pessoais, baseado no art. 5.º, X, da CF/1988 (LGL\1988\3), e a garantia instrumental para a proteção desse direito, consubstanciada na ação do *habeas data* (art. 5.º, LXXII, da CF/1988 (LGL\1988\3)).

A utilização limitada do *habeas data* até hoje pode ser explicada em razão do contexto específico de seu surgimento, vinculado à ideia de luta contra ditadura (Mendes, 2008, p. 543), bem como em razão da interpretação do STF, que estabeleceu requisitos difíceis de serem comprovados pelo impetrante, a partir de uma interpretação restrita do "interesse de agir" e do "esgotamento das vias administrativas". [16] Em parte, a aplicação limitada dessa ação advém também da própria redação do dispositivo, que prevê a possibilidade de acesso, retificação e complementação das informações, sem prever expressamente a possibilidade de cancelamento desses dados (Mendes, 2008, p. 544).

Com o reconhecimento de um direito material de proteção de dados pessoais na Constituição Federal (LGL\1988\3), abrem-se novas possibilidades para o desenvolvimento dessa ação, de modo a permitir um entendimento de sua aplicação compatível com a importância da proteção de dados pessoais na atual sociedade da informação. Sob essa perspectiva, entende-se que as hipóteses previstas art. 5.º, LXXII, da CF/1988 (LGL\1988\3) – acesso, retificação e complementação dos dados – são apenas algumas das formas processuais de proteção da privacidade, não esgotando todos os instrumentos constitucionais de tutela. Assim, reconhece--se que o *habeas data* possui virtualidades não desvendadas, cuja revelação dependerá da aplicação concreta do direito fundamental à proteção de dados, bem como da ampliação da interpretação acerca das condições processuais dessa ação (interesse de agir e esgotamento das vias administrativas). Trata-se de um instrumento poderoso, cujo potencial ainda não foi plenamente explorado pela interpretação constitucional.

Após a fundamentação desse direito, impende delinear, preliminarmente, as suas características e dimensões. O direito à proteção de dados, como uma espécie de direito à personalidade, constitui um direito tanto de caráter negativo (direito de defesa), como de caráter positivo (direito à prestação). Negativo, por delimitar uma esfera de proteção que não pode sofrer intervenção do poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito. Positivo, por ensejar também a obrigatoriedade de uma ação do Estado para garantir tal proteção.

Isso significa, sob o ponto de vista de seu caráter negativo, que nenhuma lei poderá ser promulgada de modo a eliminar esse direito fundamental, sob pena de vir a ser considerada inconstitucional e ser declarada nula. Ademais, à luz do seu caráter positivo, o direito fundamental à proteção de dados pessoais enseja um dever de proteção do Estado, tal como a edição de lei que regulamente o assunto. Nesse caso, compreende-se que o direito é garantido constitucionalmente, e que a sua densificação e conformação dependem da ação estatal.

No que diz respeito à sua eficácia, pode-se afirmar que o direito fundamental à proteção de dados tem eficácia horizontal, aplicando-se também às relações privadas. [17] Isso pode ser demonstrado pela redação do dispositivo constitucional que prevê a ação de *habeas data*: "conceder-se-á *habeas data:* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público" (art. 5.º, LXXII, da CF/1988 (LGL\1988\3)). Nesse sentido, resta clara a determinação constitucional de que tanto os bancos de dados estatais como os bancos públicos estão sujeitos à obrigação prevista no *habeas data.* Tendo em vista tratar-se de direito à personalidade, já que os dados armazenados representam a pessoa na sociedade, qualquer banco ou registro de dados pessoais deve ser entendido como público, independentemente de ser gerido por organismo privado ou estatal. À luz desse conceito, só não é público o cadastro utilizado por pessoas físicas exclusivamente para atividades pessoais ou domésticas, por exemplo, correspondência ou listas de endereços. [18] Essa eficácia horizontal pode ser demonstrada também pela sua posterior concretização no art. 43 do CDC (LGL\1990\40), que determina que os bancos de dados de consumo sejam considerados públicos.

O reconhecimento da eficácia horizontal é essencial para a proteção da personalidade em uma economia da informação pessoal, na qual a informação constitui-se como um de seus principais insumos. Tal fenômeno ultrapassa as áreas de proteção ao crédito e *marketing* direto, pois atualmente grandes empresas de varejo tomam as suas decisões de investimento referentes a estratégias, produtos e locação de pontos de venda baseadas em refinadas análises a respeito da renda, preferências e comportamento dos seus clientes (Perri 6, 2005, p. 17). Para se atingir tanto a diversificação da produção, como a personalização do *marketing* e a fidelização do cliente, faz-se necessário o armazenamento e processamento de grande quantidade de informação quase cotidiana dos consumidores e de seus

hábitos de consumo, por meio da tecnologia da informação (Schwenke, 2006). Percebe-se, assim, que a informação transformou-se em insumo da produção, possuindo um papel tão importante quanto a força de trabalho e o capital.

Vê-se, portanto, como é fundamental que a aplicação imediata do direito fundamental à proteção de dados ocorra tanto na relação dos indivíduos com o Estado, como nas relações privadas. Assim, resta claro que se a Constituição Federal (LGL\1988\3) estabeleceu de forma expressa a eficácia horizontal do instrumento *habeas data,* não há dúvidas quanto à eficácia horizontal do direito material que ele protege.

Faz-se importante destacar que o direito fundamental à proteção de dados não é um direito absoluto, podendo ser limitado, em razão da aplicação de outro direito fundamental ou preceito constitucional, aplicável ao caso concreto. [19] Isso pode ocorrer, na medida em que a informação representa um recorte da realidade social, da qual o próprio indivíduo faz parte e é interdependente. [20] Conforme afirma Alan Westin: "O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive" (1970, p. 7, trad. livre).

Por fim, pode-se afirmar que o direito fundamental à proteção de dados pessoais exige que o titular tenha efetivo controle sobre a circulação dos seus dados na sociedade, o que somente pode ser alcançado por meio da garantia dos direitos de acesso, cancelamento e retificação dos dados. Ademais, a concretização desse direito fundamental deve se pautar no cumprimento dos seguintes princípios: finalidade, transparência, esquecimento (limite temporal para o armazenamento dos dados), qualidade dos dados (exigência de um tratamento leal e lícito dos dados), consentimento e segurança física dos dados (proteção contra extravio e vazamento dos dados). A proteção do indivíduo contra a discriminação pelo processamento dos dados pessoais somente pode ser atingida com a proibição ou limitação do armazenamento de informações sensíveis e excessivas. Ademais, a efetivação do direito fundamental à proteção de dados depende do controle e fiscalização da atividade de processamento de dados por autoridade administrativa, de modo a complementar um sistema judicial de resolução de conflitos. Para a reparação dos danos morais e materiais advindos da violação do direito fundamental à proteção de dados, faz-se necessária a aplicação de um sistema de responsabilidade objetiva e solidária.

Esta exposição preliminar das características do direito fundamental à proteção de dados pessoais não tem a pretensão de exaurir o tema, o que exigiria um tratamento monográfico. Seu papel é apenas explicitar a suficiência do fundamento constitucional para este direito fundamental e possibilitar futuros desenvolvimentos dogmáticos desse direito.

5. Conclusão

Este artigo buscou rastrear o fundamento constitucional do direito fundamental à proteção de dados pessoais. Longe de estabelecer, de forma definitiva, o conteúdo e os limites desse direito, buscou-se apresentar reflexões baseadas nas evidências de sua aplicação na nossa jurisprudência e na nossa legislação. Assim, visou-se identificar as soluções que o nosso ordenamento já oferece para a proteção da privacidade.

Como visto, a inviolabilidade da intimidade e da vida privada, sob as modernas condições de processamento de dados, pressupõe a proteção do indivíduo contra a coleta, o armazenamento, o uso e a transmissão irrestrita de seus dados pessoais. Essa proteção, portanto, é abrangida pelo direito fundamental do art. 5.º, X, c/c art. 5.º, LXXII, da CF/1988 (LGL\1988\3). Esse direito fundamental atribui o poder ao cidadão de controlar livremente a divulgação, transmissão e uso de seus dados pessoais, bem como garante o tratamento leal e lícito dos seus dados, conforme as suas legítimas expectativas.

O reconhecimento do direito fundamental à proteção de dados pessoais, assim como a sua aplicação na experiência jurídica brasileira, constitui um passo necessário para a concretização da nossa Constituição. Também a aplicação dos princípios da proteção de dados, em consonância com os modernos princípios firmados internacionalmente, representam a consolidação desse direito entre nós. Trata-se de um desenvolvimento natural do direito à privacidade, que ocorre inevitavelmente a partir das novas demandas sociais originadas na sociedade da informação.

Essa evolução constitui o início de um caminho para a proteção constitucional do cidadão brasileiro na sociedade da informação. A aplicação efetiva do direito individual à proteção de dados pessoais depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, o que exigirá o empenho de diversos atores e instituições nesse processo.

Não podemos esquecer que há complexos desafios impostos pela sociedade da informação, para os quais se faz necessária a regulamentação pela via legislativa. Sem isso, pode-se comprometer tanto a segurança jurídica das atividades empresariais que envolvam o processamento de dados, como a tutela da personalidade e dos dados pessoais dos indivíduos. [21] Nesse sentido, cumpre estabelecer, por meio da edição de uma lei geral de proteção de dados pessoais, uma arquitetura regulatória, capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro setor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação. [22]

Em segundo lugar, faz-se necessário consolidar uma dogmática sobre proteção de dados pessoais no país, que delineie os contornos e as formas de garantia desse direito fundamental. Cabe à doutrina a observação e reflexão sobre a prática jurídica de modo a extrair conceitos gerais, auxiliando a aplicação do direito pelo Judiciário, que efetuará a configuração desse direito na prática cotidiana da resolução dos conflitos.

Em relação ao processo legislativo, é fundamental um pacto de não retrocesso. Para enfrentar os desafios da sociedade da informação, não podemos retroceder em relação ao patrimônio histórico da proteção de dados pessoais no mundo, que é a sua vinculação direta à proteção da pessoa e da sua dignidade. Ao contrário, temos que avançar e buscar respostas para novos desafios como aqueles propostos pelas redes sociais, as tecnologias de vigilância, a biometria, o *marketing* comportamental, a transferência internacional de dados, entre tantas outras, sempre considerando os valores fundamentais de liberdade e autonomia que inspiram esta disciplina.

Também a sociedade civil tem um importante papel nesse processo. Faz-se necessária a vigilância constante dos atos dos responsáveis pelo processamento de dados, sejam eles organismos privados ou públicos, de modo a observar se estão em consonância ou não com esse direito fundamental. Observar, vigiar e publicizar essas condutas propicia a transparência necessária para a identificação das práticas que violam a Constituição e, portanto, auxiliam no seu combate.

Somente assim, poderá a sociedade brasileira obter os benefícios econômicos e sociais advindos da revolução tecnológica, bem como concretizar uma democracia da informação que proteja, tanto a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados pessoais.

6. Bibliografia

Benjamin, Antonio Herman V.; Grinover, Ada Pellegrini et al. *Código brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.* 8. ed. Rio de Janeiro: Forense Universitária, 2005.

Bennett, Colin J. *Regulating privacy: data protection and public policy in Europe and the United States.* Ithaca, New York: Cornell University Press, 1992.

Bessa, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito.* São Paulo: Ed. RT, 2003.

Buchner, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Tübingen: Mohr Siebeck, 2006.

Canaris, Claus-Wilhelm. *Direitos fundamentais e direito privado.* Trad. Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina, 2006.

Castells, Manuel. *A galáxia da Internet. Reflexões sobre a Internet, os negócios e a sociedade.* Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Ed. Jorge Zahar, 2003.

Cueva, Pablo Lucas Murillo de la. *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática.* Madrid: Tecnos, 1990.

Doneda, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

Garfinkel, Simson. *Database nation: the death of privacy in the 21th century.* California: O'Reilly Media, 2000.

Grundmann, Stefan (org.). *Constitutional values and european contract law.* Alphen aan den Rijn: Kluwer Law International, Wolters Kluwer, 2008.

Häberle, Peter. *Verfassung als öffentlicher Prozeß: Materialien zu einer Verfassungstheorie der offenen Gesellschaft.* Berlin: Duncker & Humblot, 1978.

Higueras, Manuel Heredero. *La directiva comunitaria de protección de los datos de carácter personal.* Pamplona: Aranzadi Editorial, 1997.

Mayer-Schönberger, Victor. Generational development of data protection in Europe. In: Agre, Philip E.; Rotenberg, Marc. *Technology and privacy: the new landscape.* Cambridge: The Mit Press, 2001.

Mendes, Gilmar et al. *Curso de direito constitucional.* 2. ed. São Paulo: Saraiva, 2008.

Perez Luño, Antonio-Enrique. *Manual de informática e derecho.* Barcelona: Ariel, 1996.

Perri 6. The personal information economy: trends and prospects for consumers. In: Lace, Susane. *The glass consumer: life in a surveillance society.* Bristol: Policy Press, 2005.

Placzek, Thomas. *Allgemeines Persönlichkeitsrecht und privatrechtlicher und Informations – und Datenschutz*. Hamburg: Lit, 2006.

Rodotà, Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

Rossnagel, Alexander (org.). *Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung.* München: Beck, 2003.

Schlink, Bernhard; Pieroth, Bodo. *Grundrechte – Staatsrecht II.* Heidelberg: C.F. Müller, 2005.

Schwartz, Paul M. Privacy and democracy in cyberspace. *Vanderbilt Law Review.* vol. 52. Nashville: Vanderbilt University Law School, 1999.

Schwenke, Mathias. *Individualisierung und Datenschutz.* Wiesbaden: Deutscher Universitäts-Verlag, 2006.

Simitis, Spiros. Reviewing privacy in an information society. *University of Pensilvania Law Review.* vol. 135. p. 707. Philadelphia: University of Pensilvania, 1986-1987.

Warren, Samuel D.; Brandeis, Luis D. The right to privacy. *Harvard Law Review.* vol. 4. n. 5. Cambridge: The Harvard Law Review Association, 1890.

Westin, Alan. *Privacy and freedom.* New York: Atheneum, 1970.

1 Este artigo retoma alguns desenvolvimentos da dissertação de mestrado *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo* (2008), e os reapresenta à luz dos resultados preliminares da pesquisa desenvolvida em nível de doutoramento com o tema “Proteção de dados pessoais nas relações de consumo: desafios, limites e perspectivas para o exercício do consentimento”. A apresentação deste artigo somente foi possível com o auxílio e o apoio institucional do Deutscher Akademischer Austauschdienst – DAAD.

2 Louis Brandeis e Samuel Warren estudaram juntos no curso de direito da Harvard Law School. Quando escreveram o artigo, eram sócios na advocacia. Posteriormente, Brandeis tornou-se ministro da Suprema Corte dos EUA. O referido artigo foi considerado um dos mais citados da história norte-americana (Shapiro, 1996 apud Doneda, 2006, p. 137).

3 A lei do recenseamento visava à coleta dos dados dos cidadãos referentes à profissão, moradia e local de trabalho, com intuito de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas realizadas no país. Os dados a serem coletados por pesquisadores estavam listados na lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. Ademais, o § 9.º da norma determinava que os dados poderiam ser comparados àqueles presentes em registros públicos, com a finalidade de averiguar a veracidade das informações fornecidas, além de possibilitar a sua transmissão na forma anônima a órgãos públicos federais. Foram ajuizadas diretamente diversas reclamações constitucionais contra a lei do recenseamento, com fundamento na violação direta ao Art. 2 I GG, que protege o livre desenvolvimento da personalidade. O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração.

4 A dimensão coletiva desse direito pode ser percebida também, na medida em que a proteção de dados pessoais passa a exercer um importante papel perante a sociedade, como a preservação da democracia (Westin, 1970, p. 24).

5 A convergência em torno desses princípios pode ser demonstrada a partir da aprovação dos *Standards* Internacionais sobre Proteção de Dados Pessoais, no ano de 2009, em Madri, na 31.ª Conferência Internacional de Autoridades de Proteção de Dados. Os *Standards* podem ser acessados no seguinte endereço eletrônico: [www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/index-ides-idphp.php].

6 Esse princípio pode ser extraído do art. 6.º da Diretiva Europeia 95/46/CE.

7 A ementa do acórdão tem o seguinte teor: “ *Habeas data* – Natureza jurídica – Regime do poder visível como pressuposto da ordem democrática – A jurisdição constitucional das liberdades – Serviço nacional de informações (SNI) – Acesso não recusado aos registros estatais – ausência do interesse de agir – recurso improvido – A Carta Federal, ao proclamar os direitos e deveres individuais e coletivos, enunciou preceitos básicos, cuja compreensão é essencial a caracterização da ordem democrática como um regime do poder visível – O modelo político-jurídico, plasmado na nova ordem constitucional, rejeita o poder que oculta e o poder que se oculta. Com essa vedação, pretendeu o constituinte tornar efetivamente legítima, em face dos destinatários do poder, a prática das instituições do Estado – O *habeas data* configura remédio jurídico-processual, de natureza constitucional, que se destina a garantir, em favor da pessoa interessada, o exercício de pretensão jurídica discernível em seu tríplice aspecto: (a) direito de acesso aos registros; (b) direito de retificação dos registros e (c) direito de complementação dos registros – Trata-se de relevante instrumento de ativação da jurisdição constitucional das liberdades, a qual representa, no plano institucional, a mais expressiva reação jurídica do Estado às situações que lesem, efetiva ou potencialmente, os direitos fundamentais da pessoa, quaisquer que sejam as dimensões em que estes se projetem – O acesso ao habeas data pressupõe, dentre outras condições de admissibilidade, a existência do interesse de agir. Ausente o interesse legitimador da ação, torna-se inviável o exercício desse remédio constitucional – A prova do anterior indeferimento do pedido de informação de dados pessoais, ou da omissão em atendê-lo, constitui requisito indispensável para que se concretize o interesse de agir no habeas data. Sem que se configure situação prévia de pretensão resistida, há carência da ação constitucional do *habeas data*” (STF, RHD 22/DF, Pleno, j. 19.09.1991, m.v., rel. Min. Marco Aurélio, rel. p/ acórdão Min. Celso de Mello, *DJ* 01.09.1995).

8 Para uma análise detalhada dos limites jurídicos dos bancos de dados de crédito, ver: Bessa, Leonardo Roscoe. *O consumidor e os limites dos bancos de dados de proteção ao crédito.* São Paulo: Ed. RT, 2003.

9 Não cabe aqui uma avaliação a respeito da adequação da lei ou da suficiência das suas normas para a proteção da privacidade, nem tampouco se trata de um juízo de constitucionalidade. Antes, busca-se demonstrar os dispositivos legais que evidenciam uma preocupação com a privacidade.

10 Norma semelhante pode ser encontrada da Diretiva Europeia 95/46/CE de proteção de dados, em seu art. 15, 1: "Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento".

11 É importante ressaltar que também neste caso não se trata de um juízo de adequação, legalidade ou constitucionalidade do decreto, em relação à proteção da privacidade dos cadastrados. A análise de suas normas objetiva apenas demonstrar que existe uma preocupação com a privacidade e com o processamento de dados pessoais dos titulares. Uma análise mais detalhada sobre a suficiência da proteção exigiria um aprofundamento da pesquisa.

12 A categoria dos dados sensíveis foi prevista de forma pioneira na Convenção 108, do Conselho da Europa, de 1981, em seu art. 6.º. Esse dispositivo previu a proibição de tratamento de "categorias especiais de dados", a menos que o direito interno previsse as garantias adequadas para o seu processamento (Higueras, 1997, p. 116 e 117). O estabelecimento de um regime especial para os dados sensíveis está presente na legislação da maioria dos países europeus e na Diretiva Europeia 95/46/CE (art. 8.º), de forma a proibir ou limitar o seu processamento.

13 Conforme afirma, Peter Häberle: "As Constituições surgiram essencialmente da experiência, segundo a qual o poder muitas vezes é utilizado contra os cidadãos. As formas de abusos de poder transformam-se; a Constituição deve também reagir por meio de novas formas que correspondam a essa mudança (…)" (1978, p. 67, trad. livre).

14 Segundo Peter Häberle, a Constituição institucionaliza experiências e tem como característica principal a sua abertura, isto é, deve deixar espaço para desenvolvimento do espírito humano e de sua história. Assim, a interpretação constitucional deve ser um processo aberto e plural, do qual a toda a sociedade deve poder participar – o que ele denomina de sociedade aberta dos intérpretes da Constituição (1978, p. 123).

15 Vale destacar que a mudanças de interpretação constitucional, em razão da necessidade de concretização de novos direitos, não acarreta um julgamento negativo sobre a interpretação do passado. Afinal, bom ou ruim somente podem ser julgamentos válidos no âmbito de um mesmo espaço temporal: "O que é bom hoje não faz o que era ontem ruim" (Häberle, 1978, p. 89, trad. livre).

16 Essa interpretação restrita pode ser vista no acórdão do STF proferido em recurso em *habeas data* (RHD 22/DF), no qual se decidiu, por maioria, pelo desprovimento da ação em razão da falta de interesse de agir. Restaram vencidos o rel. Min. Marco Aurélio, e o Min. Sepúlveda Pertence, que davam provimento ao recurso, ao defender a existência de interesse de agir do impetrante com base na comprovação, nos próprios autos, da contrariedade da autoridade em conceder acesso aos dados pessoais do impetrante.

17 Não desconhecemos a complexa discussão em torno da aplicação imediata dos direitos fundamentais às relações privadas. Conforme afirma Claus-Wilhelm Canaris, a relação entre a Constituição e o direito privado representa uma verdadeira "problemática do século" (2006, p. 20). O debate na Alemanha centrou-se majoritariamente na discussão acerca da aplicação desses direitos às relações privadas e se tal aplicação dar-se-ia de forma indireta, por meio de cláusulas gerais do direito privado, ou direta, sem qualquer mediação de conceitos de direito privado. Os defensores de um efeito mediato dos direitos fundamentais afirmam que o sistema de valores da Constituição influencia o direito civil, por meio de uma irradiação realizada pelas cláusulas gerais de direito privado, entendidas como "pontos de penetração" dos direitos fundamentais no direito civil. Assim, essa corrente entende que a liberdade e a igualdade são melhor preservadas quando os direitos fundamentais não são utilizados para resolver em concreto os litígios do direito civil, mas funcionam como parâmetros de influência e irradiação. Por outro lado, a favor de um efeito imediato para terceiros, argumenta-se que os direitos fundamentais são a base de toda a sociedade humana (Art. 1, Nr. 2 GG) e que a transformação do Estado de Direito de liberal para social demonstrou que as ameaças à liberdade também podem partir das forças sociais, tais como empresas e organizações de classe, entre outros (Schlink; Pieroth, 2005, p. 44 e 45). Stefan Grundmann afirmou, no entanto, que apesar do intenso debate e dos entendimentos doutrinários divergentes, é difícil verificar uma diferença real entre ambos os entendimentos. (Grundmann, 2008, p. 7) Não aprofundaremos aqui essa ampla discussão sobre a aplicação imediata dos direitos fundamentais às relações privadas, pois entendemos que a Constituição Federal (LGL\1988\3) já estabeleceu essa eficácia de forma expressa em relação ao *habeas data.*

18 Esse é o entendimento que nos parece mais adequado em face da efetividade do direito à privacidade numa sociedade da informação. Essa interpretação também pode ser depreendida do art. 3.º, 2, da Diretiva Europeia 95/46/CE de proteção de dados pessoais: "Art. 3.º (…) 2. A presente directiva não se aplica ao tratamento de dados pessoais: (…) – Efectuado por uma pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas".

19 Como um exemplo de limitação do direito à privacidade em face do princípio da publicidade previsto no art. 37, *caput*, da CF (LGL\1988\3), vale mencionar a decisão do Plenário do STF, que negou provimento ao agravo regimental interposto contra decisão monocrática do presidente do Tribunal (Segundo AgRg na SS 3.902/SP, j. 09.06.2011, v.u., rel. Min. Ayres Britto, *DJe* 17.06.2011). Decidiu-se, no referido julgamento, que a divulgação dos vencimentos brutos de servidores, a ser realizada pelo Estado, constituiria interesse coletivo, sem implicar violação à intimidade e à segurança deles, uma vez que esses dados se referem a agentes públicos em exercício nessa qualidade. Afirmou--se, ademais, que não seria permitida a divulgação do endereço residencial, CPF e RG de cada um, mas apenas de seu nome e matrícula funcional.

20 Não constitui objeto deste artigo analisar os limites do direito à privacidade em relação a outros preceitos constitucionais, o que exigiria um tratamento monográfico.

21 No mesmo sentido, Paul Schwartz afirma ser necessária, para a eficácia desse direito, a institucionalização pelo Estado de mecanismos que possibilitem o exercício da autonomia do indivíduo (1999, p. 1162).

22 O anteprojeto de lei apresentado pelo Ministério da Justiça e posto em consulta pública em novembro de 2010 nos parece extremamente adequado para essa finalidade, por estabelecer um marco normativo geral sobre proteção de dados pessoais com direitos e princípios fundamentais e por abarcar os setores público e privado.